МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

М.В. Афанасьєв

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**"КІБЕРБЕЗПЕКА"**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *Кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 1 від 26.08.2019 р.

Розробник(-и):
Корольов Р.В., к.т.н., доцент кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Анотація навчальної дисципліни:

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів. В даний час набули широкого поширення засоби і методи несанкціонованого доступу і отримання інформації в кіберпросторі. Вони знаходять все більше застосування не тільки в діяльності державних правоохоронних органів розвинених держав, а й в діяльності хакерів і різного роду злочинних кіберугрупувань.

Необхідно пам'ятати, що природні канали витоку інформації утворюються спонтанно, в силу специфічних обставин, що склалися на об'єкті захисту. Що стосується штучних каналів витоку інформації, то вони створюються навмисно із застосуванням активних методів і способів отримання інформації. Активні способи припускають навмисне створення технічних каналів витоку інформації з використанням спеціальних технічних засобів. До них можна віднести незаконне підключення до каналів, проводам і лініям зв'язку, високочастотне нав'язування і опромінення, установка в технічних засобах і приміщеннях відеокамер, мікрофонів і телефонних закладних пристроїв, а також несанкціонований доступ до інформації, що обробляється в автоматизованих системах тощо.

Тому особливу роль і місце в діяльності по захисту інформації займають заходи щодо створення комплексного захисту, що враховують загрози національній і міжнародній безпеці і стабільності, в тому числі суспільству, особистості, державі, демократичних цінностей і суспільних інститутів, суверенітету, економіці, фінансовим установам, розвитку держави.

Мета навчальної дисципліни: метою викладання дисципліни "Комплексні системи захисту інформації" є навчання студентів принципам побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації.

Курс	**4**	
Семестр	**1**	
Кількість кредитів ECTS	**4**	
Аудиторні навчальні заняття	**лекції**	**30**
	семінарські, практичні	**–**
	лабораторні	**30**
Самостійна робота		**60**
Форма підсумкового контролю	**залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Основи криптографічного захисту	Основи технічного захисту інформації
Менеджмент інформаційної безпеки	Організаційне забезпечення захисту інформації
Безпека в інформаційно-комунікаційних системах	Захист систем електронної комерції та мультисервісних систем

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки
Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах
Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем	Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; здійснювати оцінку захищеності ІТ систем та мереж; використовувати інструментальні засоби оцінки наявних вразливостей; оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж
Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов	Виконувати налаштування інформаційних систем та комунікаційного обладнання; виконувати захист інформаційних систем від комп'ютерних вірусів; забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; організовувати процес створення планів неперервності бізнесу; приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ

3. Програма навчальної дисципліни

Змістовий модуль 1.Нормативно-правові аспекти побудови КСЗІ. Захист інформації від технічних каналів витоку

Тема 1.Нормативно-правове забезпечення в сфері інформаційної безпеки

Основні законодавчі акти, що регламентують інформаційну безпеку в Україні. Нормативно-правове забезпечення технічного захисту інформації (ТЗІ) в Україні. Вимоги нормативних документів технічного захисту інформації. Вимоги до захисту інформації в інформаційно-комунікаційних системах (ІКС). Ліцензування діяльності в галузі ТЗІ. Порядок здійснення контролю за дотриманням ліцензійних умов. Основні положення міжнародних стандартів управління інформаційною безпекою. Міжнародні стандарти управління інформаційної безпекою (Європа, США, Великобританія). Сімейство міжнародних стандартів ISO 15408, 27xxx.

Тема 2. Захист інформації в інформаційно-комунікаційних системах від витоку технічними каналами

Основні поняття з витоку інформації *в інформаційно-комунікаційних системах*. Класифікація каналів витоку. Загальна модель технічного каналу витоку інформації. Оптичні канали витоку інформації та методи захисту. Основи розповсюдження оптичних сигналів. Класифікація та характеристика оптичних та оптоелектронних засобів технічної розвідки. Методи захисту від витоку оптичними каналами.

Тема 3. Радіоканали витоку інформації.

Витік інформації радіоканалами в ІКС. Радіозакладні пристрої та методи їх маскування. Загрози несанкціонованого застосування засобів радіозв'язку в ІКС.

Тема 4. Акустичні канали витоку інформації та методи захисту

Джерела акустичних сигналів на об'єктах інформаційної діяльності. Основні засоби технічної розвідки акустичних сигналів. Класифікація акустичних каналів витоку інформації. Звукоізоляція елементів приміщення. Інженерне обладнання об'єкту.

Тема 5. Побічні електромагнітні випромінювання (ПЕМВ) засобів обчислювальної техніки (ЗОТ)

Фізичні основи утворення ПЕМВ в ЗОТ. Параметри інформаційних сигналів, що циркулюють в ЗОТ. Технічні канали витоку в ЗОТ за рахунок ПЕМВ.

Тема 6. Загрози інформації в сучасних ІКС.

Модель загроз інформації в ІКС. Класифікація загроз в кіберпросторі, інформаційної безпеки та безпеки інформації. Синергетичний підхід щодо оцінювання загроз на ІКС.

Тема 7. Канали витоку при експлуатації ЕОМ

Види та природа каналів витоку інформації. Оцінка рівня ПЕМВ. Методи і засоби НСД по технічним каналам

Змістовий модуль 2. Створення КСЗІ в інформаційно-телекомунікаційних системах

Тема 8. Формування загальних вимог до КСЗІ в ІКС.

Призначення КСЗІ. Суб'єкти та об'єкти КСЗІ. Послідовність робіт зі створення КСЗІ.

Порядок проведення обстеження середовищ функціонування ІТС. Порядок оформлення моделі загроз, моделі порушника. Формування завдання на створення КСЗІ. Порядок розроблення, впровадження, експертні випробування, супроводження КСЗІ від несанкціонованих дій в ІС, ТС, ІКС.

Служба захисту інформації (СЗІ). Порядок створення, призначення та структура СЗІ. Завдання та функції СЗІ. Порядок організації робіт СЗІ.

Тема 9.Етапи побудови КСЗІ.

Порядок розробки політики безпеки (ПБ) інформації в ІКС. Основні положення ПБ в КСЗІ. Порядок документального оформлення ПБ. Розробка технічного завдання (ТЗ) на створення КСЗІ. Загальні вимоги та порядок розробки ТЗ на КСЗІ в АС. Вимоги до змісту розділів ТЗ. Порядок оформлення ТЗ. Порядок розробки проекту КСЗІ. Ескізний проект КСЗІ. Технічний проект КСЗІ. Робочий проект КСЗІ. Загальні вимоги до порядку введення КСЗІ в дію. Підготовка КСЗІ до введення в дію. Порядок проведення попередніх випробувань. Порядок проведення дослідної експлуатації. Основні положення проведення Державної експертизи КСЗІ. Порядок організації та проведення Державної експертизи КСЗІ.

Тема 10. Система управління інформаційною безпекою підприємства

Стандарти управління інформаційною безпекою (СУІБ). Методика формування нормативних, розпорядчих та методичних документів в процесі впровадження та функціонування СУІБ. Організаційна структура служби інформаційної безпеки. Варіанти оброблення ризиків. Вибір методу оброблення ризиків. Програмна підтримка аналізу ризиків. Оцінка відповідності СУІБ своєму призначенню відповідно до вимог діючих стандартів та нормативних документів.

Теми лабораторних робіт

Лабораторна робота 1. Дослідження стійкості парольного захисту

Лабораторна робота 2. Дослідження стійкості точок доступу бездротової мережі Wi-Fi

Лабораторна робота 3. Дослідження ефективних методів захисту від експлойтів

Лабораторна робота 4. SQL-ін’єкції та методи боротьби з ними

Лабораторна робота 5. Аутентифікація користувачів на основі токенів безпеки

Лабораторна робота 6. Підсистема управління доступом

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі колоквіуму як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються; ступінь засвоєння фактичного матеріалу навчальної дисципліни; ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються; вміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв'язанні задач, проведенні розрахунків у процесі виконання індивідуальних завдань та завдань, винесених на розгляд в аудиторії; логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки; арифметична правильність виконання індивідуального та комплексного розрахункового завдання; здатність проводити критичну та незалежну оцінку певних проблемних питань; вміння пояснювати альтернативні погляди та наявність власної точки зору, позиції на певне проблемне питання; застосування аналітичних підходів; якість і чіткість викладення міркувань; логіка, структуризація та обґрунтованість висновків щодо конкретної проблеми; самостійність виконання роботи; грамотність подачі матеріалу; використання методів порівняння, узагальнення понять та явищ; оформлення роботи.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на практичних та семінарських заняттях.

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час заліку, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

(вказати засоби оцінювання згідно з технологічною картою)

Теми змістового модуля				Лекційні заняття	Захист лабораторних робіт	Експрес-опитування	Поточні КР	Усього
	1	**Тема 1**	1 тиждень	1				1
		Тема 1	2 тиждень	1	5	3		9
		Тема 1	3 тиждень	1				1
		Тема 2	4 тиждень	1	5	3		9
		Тема 3	5 тиждень	1			11	12
		Тема 4	6 тиждень	1		3		4
		Тема 5	7 тиждень	1	5			6
		Тема 6	8 тиждень	1		3		4
		Тема 7	9 тиждень	1			11	12
		Тема 7	10 тиждень	1	5	3		9
	2	**Тема 8**	11 тиждень	1				1
		Тема 8	12 тиждень	1		3		4
		Тема 9	13 тиждень	1	5			6
		Тема 10	14 тиждень	1		4	11	16
		Тема 10	15 тиждень	1	5			6
Усього				15	30	22	33	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

5.1 Основна

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);
2. Закон України “Про захист персональних даних” (2010)
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
4. Закон України “Про національну безпеку (2018)
5. Стратегія кібербезпеки України” (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
14. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.
15. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації вкомп'ютерних системах від несанкціонованого доступу.
16. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації віднесанкціонованого доступу.
17. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексноїсистеми захисту інформації в інформаційно-телекомунікаційній системі.
18. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічногозавдання на створення комплексної системи захисту інформації в АС.
19. НД ТЗІ 1.6-004-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація зобмеженим доступом, що становить державну таємницю.
20. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація зобмеженим доступом, що не становить державної таємниці

5.2 Додаткова

21.ISO/IEC 27001. "Информационные технологии. Методы обеспечениябезопасности. Системы управления информационной безопасностью.

22. ISO/IEC 27002. "Информационные технологии. Методы обеспечениябезопасности. Практические правила управления информационнойбезопасностью."

23. ISO/IEC 27005. "Информационные технологии. Методы обеспечениябезопасности. Управление рисками информационной безопасности

5.3 Інформаційні ресурси мережі інтернет

24. http://bezopasnost.biz

25. http://dstszi.gov.ua